Amendments to the Claims:

This listing of the claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended). A method of generating an authentication key for an electronic document file representative of a document, the method comprising:

providing the electronic document file as an initial digital file;

submitting the initial digital file without intervening transformation directly to a predetermined halftoning process, thereby to generate a digital halftone file, wherein the halftoning process creates a multi-plane bitmap defined by specific placement and size of different colored ink drops; and

submitting the digital halftone file to a predetermined mathematical process to thereby generate the authentication key, wherein the mathematical process includes mathematically combining the multi-plane bitmap to create the authentication key.

2. (Previously Presented). The method of claim 1, and further comprising printing the digital halftone file to provide a tangible copy of the document, and printing with the tangible copy of the document a visible representation of the authentication key.

3. (Original). The method of claim 1, and further comprising displaying the digital halftone file on a user display to provide a visible copy of the document and the authentication key.

4. (Original). The method of claim 1, and wherein the halftoning process is based, at least in part, on an error diffusion halftoning algorithm.

5. (Original). The method of claim 1, and wherein the halftoning process is based, at least in part, on one of a matrix-based halftoning algorithm, a pattern-based halftoning algorithm, or an ordered-dither halftoning algorithm.

6. (Original). The method of claim 1, and wherein the predetermined mathematical process is a summation process.

7. (Currently Amended). A method of authenticating an electronic document file representative of a document, the method comprising:

receiving the electronic document file as an initial received digital file;

submitting the initial received digital file without intervening transformation directly to a predetermined halftoning process, thereby to generate a digital halftone file defined by a plurality of discrete digital values, wherein the halftoning process creates a multi-plane bitmap defined by specific placement and size of different colored ink drops;

submitting the digital halftone file to a predetermined mathematical process involving each of the plurality of discrete digital values in the digital halftone file, thereby to produce a receiver-generated authentication key for the initial received digital file, wherein the mathematical process includes mathematically combining the multi-plane bitmap to create the authentication key; and

using the receiver-generated authentication key to verify the authenticity of the initial received digital file relative to the electronic document file.

8. (Previously Presented). The method of claim 7, and wherein the step of using the receiver-generated authentication key comprises:

receiving a sender-generated authentication key for the electronic document file;

comparing the sender-generated authentication key to the receiver-generated authentication key; and

accepting the authenticity of the initial received digital file relative to the electronic document file, when the sender-generated and the receiver-generated authentication keys are identical.

9. (Original). The method of claim 7, and wherein the halftoning process is based, at least in part, on an error diffusion halftoning algorithm.

10. (Original). The method of claim 7, and wherein the halftoning process is based, at least in part, on one of a matrix-based halftoning algorithm, a pattern-based halftoning algorithm, or an ordered-dither halftoning algorithm.

11. (Original). The method of claim 7, and wherein the predetermined mathematical process is a summation process.

12. (Original). The method of claim 9, and wherein the electronic document file is received from a sender via a network.

13. (Original). The method of claim 10, and wherein the sender authentication key is received via one of telephone or facsimile.

14. (Currently Amended). A system to generate an authentication key for an electronic document file representative of a document, the system comprising:

a processor; and

a computer readable memory device readable by the processor, the computer readable memory device containing a series of computer executable steps configured to cause the processor to:

retrieve a copy of the electronic document file as an initial digital file;

submit the initial digital file without intervening transformation directly to a predetermined halftoning process, thereby to generate a digital halftone file, wherein the halftoning process creates a multi-plane bitmap defined by specific placement and size of different colored ink drops;

submit the digital halftone file to a predetermined mathematical process to thereby generate the authentication key, wherein the mathematical process includes mathematically combining the multi-plane bitmap to create the authentication key; and

store a copy of the authentication key in the computer readable memory device.

15. (Original). The system of claim 14, and wherein the processor and the computer readable memory device are resident within a document printing device.

16. (Original). The system of claim 15, and wherein the series of computer executable steps are further configured to cause the processor to print a tangible copy of the halftone image file as the document, and to include the authentication key on the tangible copy of the halftone image file.

17. (Original). The system of claim 14, and wherein the computer readable memory is configured to store, at least temporarily, a copy of the electronic document file as the initial digital document file.

18. (Previously Presented). The system of claim 15, and further comprising a user display, and wherein the series of computer executable steps are further configured to cause the processor to display the authentication key on the user display.

19. (Currently Amended). A system for authenticating an electronic document file representative of a document, the system comprising:

a processor;

a computer readable memory device readable by the processor and configured to receive the electronic document file as an initial received digital file, the computer readable memory device containing a series of computer executable steps configured to cause the processor to:

store the initial received digital file in the computer readable memory device;

submit the initial digital file without intervening transformation directly to a predetermined halftoning process, thereby to generate a digital halftone file defined by a plurality of discrete digital values, wherein the halftoning process creates a multi-plane bitmap defined by specific placement and size of different colored ink drops;

submit the digital halftone file to a predetermined mathematical process involving each of the plurality of discrete digital values in the digital halftone file to thereby produce a receiver-generated authentication key for the initial received digital file, wherein the mathematical process includes mathematically combining the multi-plane bitmap to create the authentication key; and

display a copy of the receiver-generated authentication key on one of a printer or a user display.

20. (Previously Presented). The system of claim 19, and further comprising a modem configured to process the initial received digital file from a sender and communicate the initial received digital file to the computer readable memory device by way of the processor.

21. (Previously Presented). The system of claim 19, and further comprising one of a telephone or a facsimile machine configured to receive a sender -generated authentication key for the electronic document file capable of being compared to the receiver-generated authentication key to authenticate the initial received digital file relative to the electronic document file.

22. (Original). The system of claim 19, and wherein the processor and the computer readable memory device are resident within a document printing device.

23. (Currently Amended). An system to authenticate an electronic document file, the system comprising:

a sender computer configured to provide the electronic document file in the form of a sender initial digital file;

a sender printer configured to:

receive the sender initial digital file;

submit the sender initial digital file without intervening transformation directly to a predetermined halftoning process, thereby to generate a first digital halftone file, wherein the halftoning process creates a multi-plane bitmap defined by specific placement and size of different colored ink drops;

submit the first digital halftone file to a predetermined mathematical process to thereby generate a sender authentication key, wherein the mathematical process includes mathematically combining the multi-plane bitmap to create the authentication key; and

display the sender authentication key to a sender;

a receiver computer configured to receive the electronic document file from the sender as a receiver initial digital file;

a receiver printer configured to:

receive the receiver initial digital file;

submit the receiver initial digital file without intervening transformation directly to the predetermined halftoning process, thereby to generate a second digital halftone file;

submit the second digital halftone file to the predetermined mathematical process to thereby generate a receiver authentication key; and

display the receiver authentication key to a receiver.

24. (Previously Presented). The system of claim 23, and further comprising a network connection configurable to allow the sender computer to send the sender initial digital file to the receiver computer.

25. (Previously Presented). The system of claim 23, and further comprising one of:

a sender telephone and a receiver telephone together allowing the sender to communicate the sender authentication key to the receiver; or

a sender facsimile machine and a receiver facsimile machine together allowing the sender to communicate the sender authentication key to the receiver.